マルチメディア通信と分散処理 111－18
コンピュータセキュリティ 20－18
（２００３．２．２７）

予防／回復機能を有する自律型セキュリティ管理システム (1)

面 和成　　鳥居 悟

㈱富士通研究所
〒211－8588 川崎市中原区上小田中4－1－1
E-mail: {komote, pro104}@labs.fujitsu.com

あらまし ネットワークシステムを安全に保つためのセキュリティ運用管理作業を支援する技術は数多く提案されている．しかし，ネットワークやパソコンの普及･高機能化に伴い，ネットワークシステムが大規模かつ複雑になり，管理者の人手によるセキュリティ運用管理には限界が見えはじめている．
本研究では，不正アクセス等の脅威からネットワークシステムの安全性を自律的に維持することを目指し，様々な情報をもとに最善な対策を判断／命令する自律型セキュリティ管理システムのフレームワークを提案する．そこで，まず，管理者やネットワークシステムを取り巻く現状を整理し，セキュリティ管理のための要件をまとめる．これらの要件を解決するための自律性とは何かを定義し，予防／回復機能の必要性を述べる．そして最後に，自律型セキュリティ管理システムのモデルを提案し，提案システムが自律性を有することを言及する．

An Autonomic Security Management System with Prevention and Recovery (1)

Kazumasa OMOTE　　Satoru TORII

Fujitsu Laboratories Ltd.
Kamikodanaka 4-1-1, Nakahara, Kawasaki, Kanagawa 211-8588 Japan
E-mail: {komote, pro104}@labs.fujitsu.com

Abstract Many tools for security management are proposed to keep a network system secure. However, it will be hard for a security administrator to manage a network system because it becomes large and complicated by developed and spread network/PC.
In this paper, we propose a framework of autonomic security management system, which manages to keep a network system secure and prevents it from intrusion by decision the best measure based on information. We mention the state of network system and list some requirements for security management. Then, we define the autonomy to solve these requirements and state the necessity of prevention and recovery. Finally, we propose a security management system model and mention that our model is autonomic.

1. はじめに

近年，ネットワークサービスの多様化に伴い，ネットワークシステムが大規模かつ複雑になってきている．このため，従来のようなシステム管理者による手動の対策実施やファイアウォールによる対策などでは，ネットワークシステムの安全性確保が困難なものとなっている．

このような背景において，ネットワークシステムのセキュリティ管理に必要なこととして，(1) 最新のセキュリティ関連情報から適切なものをすばやく入手すること，(2) ネットワークシステムの構成等に関する情報を正確に把握すること，(3) これらの情報をもとに迅速かつ適切に対策を導出すること，および，(4) 導出された複数の対策に対してその時点で最適な対策を選択し実施すること，が挙げられる．

現状では，ツールの連携等によって，ネットワークシステムのセキュリティが向上されつつある．しかしながら，相変わらずこれらの最終的な判断は全て管理者自身にゆだねられており，この管理者の作業コストは膨大なものとなっている．

本稿では，不正アクセス等の脅威からネットワークシステムの安全性を自律的に維持することを目指し，様々な情報をもとに最善な対策を判断／命令する自律型セキュリティ管理システムのフレームワークを提案する．

以下，2章でシステム管理者やネットワークシステムを取り巻く現状を整理し，3章でセキュリティ管理のための要件を挙げる．4章では関連技術･研究についてまとめ，現状技術では解決できていないことを示し，5章では我々が目指している自律性について述べる．6章では自律型セキュリティシステムモデルを提案し，それらのケーススタディを7章で示す．8章では提案システムが自律性を満たしているかについて検討し，最後に9章でまとめと今後の課題を示す．

2. 管理者やシステムを取り巻く現状

(1) セキュリティ関連情報の氾濫
種々のセキュリティホール情報は1日に数十件も報告されており，また，主要なセキュリティ関連メーリングリストでは様々な意見交換が行われており，全体として1日に数百件の情報が流れている．これらの全ての情報を把握し熟知するのが非常に困難なものとなっている．

(2) システムの構成要素の多様化
あるサービスを提供しているサーバマシンが関西と関東のそれぞれのセンタに分散化されていたり，あるいは，そのサービスを提供するためには複数のソフトウェアがインストールされていたりする．それゆえに，どこにどのようなサービスを提供している計算機があり，そのサービスを提供するためにどのようなソフトウェアがインストールされているかが，単純には分からなくなっている．

(3) 攻撃手法や被害の拡散速度の高速化
通信性能や処理性能の向上に伴い，被害の蔓延速度が高速化している．単純なひとつのコンピュータワームを契機に，わずか数時間で世界中のネットワークが麻痺する危険性がある．

(4) 利用形態や被害形態の多様化
これまでは，単にネットワークの出入り口にて悪意の通信をファイアウォール等で制限することが主なセキュリティ対策であった．しかし，コンピュータワームの被害事例が示すように，計算機の利用形態の変化に伴い，侵入･攻撃手口が多岐にわたるものとなっており，決められたある特定の対策を単純に実施するだけでは不十分なものとなっている．

3. セキュリティ管理のための要件

本章では，ネットワークシステムのセキュリティ管理に必要なことを以下のように定義する．セキュリティ管理の概念図を図1に示した．

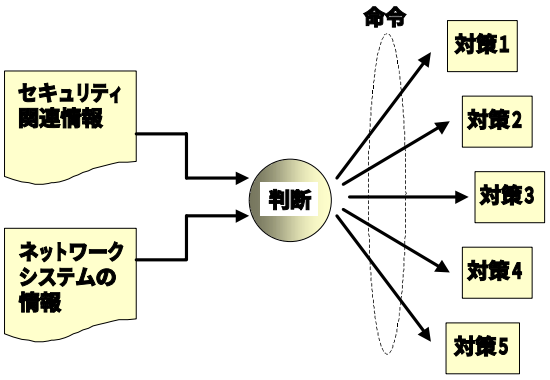

図1：セキュリティ管理の概念図

(1) 最新のセキュリティ関連情報から適切なものをすばやく入手すること
セキュリティ関連情報には，セキュリティホール情報やパッチ関連情報等が含まれる．ネットワ

ークシステムを常に安全に維持するためにはセキュリティ関連情報をすばやく入手し，取捨選択をする必要がある．

(2) **ネットワークシステムの構成等に関する情報を正確に把握すること**

ネットワークシステムの情報には，マシン情報，ネットワーク情報，機器構成情報，診断情報等の情報が含まれる．対象となるマシンを安全にするためには，対象マシンがどこにあり，何のソフトウェアがインストールされているかの情報を取得して整理しておく必要がある．

(3) **迅速かつ適切に対策を導出すること**

少しでもマシンを危険な状態に放置しないように，また，被害の拡大を少しでも抑えるために，対策を迅速かつ適切に導出する必要がある．

(4) **複数の対策に対して最善な対策を選択し実施すること**

単に事象の解決を図るためだけでなく，ネットワークシステム全体のセキュリティを維持するために，複数の対策の中でどの対策が最善かを判断して実施する必要がある．また，ネットワークシステムのどこで対策を行うのが最善なのかを判断することも必要である．

4. 関連技術・研究

本章では，セキュリティ管理に関する技術および研究をいくつか紹介し，それらの課題を示す．

4.1. 自動パッチ適用システム

文献[1]は，自動パッチ適用に関するもので，パッチサーバがパッチ適用に必要なDBを参照して，パッチ適用が必要なクライアントシステムに対し自動かつ適切に最新のパッチを適用するシステムである．しかし，パッチを適用できないマシンやパッチがないマシンは脆弱のままとなり，パッチ適用以外の対策はなされない．

4.2. 運用管理システム

運用管理システムはシステムの安定稼働を目的とし，ネットワークの構成等に関する情報をシステム管理者に通知するものである．しかし，それらの情報からシステムが脆弱であるかどうかの判断や何をすべきかの判断までは行わない．

4.3. 対策技術

FW－IDS連携は，IDS で検知した情報をファイアウォール（FW）にフィードバックさせて，FW のルールを更新して動的に防御する技術である．

文献[2,3]は，Web サーバを防御するシステムに関するもので，ファイアウォール等で防御できない不正なHTTPリクエストをあらかじめフィルタリングすることによって，Web サーバへの不正なアクセス等を防御するシステムである．

文献[4]は，通常アクセスするマシンが限定されているという仮定のもと，新しいマシンに対するアクセススピードを遅らせることによって，ウィルス拡散を抑えるアイディアを提案している．

これらの技術は，個々の対策や状況に応じて変化させられるべきものである．

4.4. 統合型セキュリティ管理

統合型セキュリティ管理とは，ウィルス対策やファイアウォール，IDS 等のいくつかのツールを統合し，セキュリティポリシに基づいて集中管理を可能とするものである．しかし，状況や対策が変化すれば，それに応じてセキュリティポリシが見直されなければならない．

5. 自律性について

本章では，関連技術･研究では満たされていない“自律性”について触れる．

5.1. 定義

本稿における‘自律性’とは，3章で示したセキュリティ管理のための要件を全て満たす必要があり，すなわち，

“最新のセキュリティ関連情報から適切なものをすばやく入手し，かつ，ネットワークシステムの構成等の情報を正確に把握し，それらの情報をもとに迅速かつ適切に対策を導出し，その中で最善な対策を選択し実施することを自動的に行う性質”

と定義する．

5.2. 自律であるための課題

4章で紹介した従来の関連技術･研究は，3章で示したセキュリティ管理のための要件を部分的に満たすものかもしれないが，全てを満たしてはいない．5.1 の定義から，システムが自律であるための課題は，3 章で示したセキュリティ管理のための要件の全てを自動的に満たすことである．

5.3. 複数の対策内容について

導出される複数の対策は，ネットワークシステムへの脅威から大きく2つに分けることができる．すなわち，ネットワークシステムへの脅威には，アタックやウィルス感染等による被害発生という要素と被害拡散という要素の2つがある．それらの要素を防止するためには，被害を受けないように予防を万全にしておくこと，及び，被害後に被害拡散を防止して回復させることの両方が必要である．

- **予防（事前対策）**

セキュリティホール情報やアタック／ウィルス情報等およびネットワークシステム内の様々な情報からの判断をもとに，被害を受けないようにする対策である．これにより，アタックおよびウィルス感染等をさせないようにできる．

- **回復（事後対策）**

マシンの挙動やネットワークの通信内容等から被害を受けたかどうかの判断情報をもとに，被害を拡大しないようにする対策である．これにより，アタックおよびウィルス感染等をすばやく回復させることができる．

6. 提案システムモデル

4章では，自律の対象となる対策が予防と回復の2つに分類されることを言及した．そこで本章では，予防機能と回復機能を有する自律型セキュリティ管理システムのフレームワークを提案する．

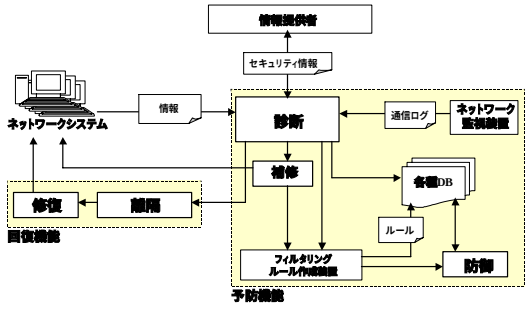

図2：システム構成図

6.1. システム構成

セキュリティ管理システムの構成を図2に示した．情報提供者，ネットワークマシン，予防機能および回復機能から構成されている．

情報提供者： 情報提供者は，Webページ等からセキュリティホール情報やパッチ関連情報などの様々な情報を公開する．実際には，複数の情報提供者が存在し，重複している情報や信頼性の低い情報も数多く存在する．

ネットワーク監視装置： ネットワークの通信を監視し，不正な通信に反応してログなどの結果を生成する装置である．IDS等がこれに相当する．

フィルタリングルール作成装置： セキュリティホール情報やアタック情報等からそれらを防ぐためのルールを作成する装置である．

ネットワークマシン： 予防および回復の対象となるネットワークシステム内のマシンである．1つのネットワークシステムに複数のマシンが存在する．ネットワークマシンから，各マシン情報，ネットワーク構成，機器構成，診断情報等の情報を取得できる．

各種ＤＢ： フィルタリングＤＢ，パッチ適用ＤＢ，ルールＤＢ，アタック／ウィルスＤＢ，マシンプロファイルＤＢ，機器構成ＤＢがある．

6.2. 機能

予防機能と回復機能のそれぞれの詳細について説明する．

6.2.1 予防機能

予防機能とは，ネットワークシステムを常に安全な状態にするために最善を尽くし，アタックおよびウィルス感染等の被害を受ける確率を最小化する機能である．予防機能は，回復機能に比べて重要である．なぜなら，ネットワークシステムの被害からの回復はそれの予防に比べて圧倒的にコストがかかるからである．予防機能の構成要素として以下の機能が考えられる．

診断： これは，ネットワークシステムを総合的に診断する機能である．情報提供者からの情報収集，ネットワークマシンの診断，不正な通信のチェックおよび各種ＤＢの参照を行い，それらの情報をもとに最善の判断を行い，補修，同定／離隔もしくはフィルタリングルールの作成を実行する．また，実際に被害を受けた場合，被害に関する情報をＤＢに格納し，それと同時に回復機能に送信する．このＤＢによって，被害に関する情報が他のネットワークシステムにフィードバックでき，同じ被害が出ないように予防できる．

補修： これは，既知のセキュリティホールへに対してパッチ等を適用する機能である．診断機能に

よってパッチを適用する必要があると判断された場合パッチを適用し，その後マシンの動作検証までを行う．

防御： これは，何らかの事情で補修しない，もしくは，補修できないネットワークシステム内のマシンが被害を受けないようにフィルタリングによって防御する機能である．フィルタリングルールに基づいて防御を行う．

6.2.2 回復機能

回復機能とは，アタックおよびウィルス感染等の被害が発生した場合，その被害を最小限に抑え，すばやく回復させる機能である．たとえ，最善の予防策を施したとしても，新たなセキュリティ問題が発見されるなど外部環境の変化により，最善の予防策は変化するので，このような回復機能も重要である．回復機能の構成要素として，以下の機能が考えられる．

離隔： これは，診断機能によって同定されたネットワークシステム内の被害範囲をもとに，同定された範囲の通信を静的もしくは動的に制限する機能である．

修復： これは，被害を受けたマシンを修復する機能である．離隔機能からの離隔完了通知を受け取ると，被害を受けたマシンの修復を行う．

7. ケーススタディ

本章では，6つのケーススタディを示すことによって提案するシステムの妥当性を示す．また，このケーススタディによって，提案システムの機能の連携を示す．

7.1. セキュリティホールが公表された場合

未公表なものも含むセキュリティホール情報が公表された場合，以下の動作を行う．

1. セキュリティ関連情報とネットワークシステムの情報から，脆弱となるマシンがどれかを判断する．ただし，そのセキュリティ関連情報が正当であるかについては何らかの方法で検証する必要がある．
2. セキュリティホールの危険度を考慮し，防御対象となるマシンを判断する．
3. フィルタリングルールを作成することによって，セキュリティホールへのアタックから防御する．

7.2. パッチが公開された場合

新たなパッチが公開された場合，以下の動作を行う．

1. セキュリティ関連情報とネットワークシステムの情報から，パッチ適用が必要なマシンがどれかを判断する．
2. パッチを充てる必要があると判断された場合，対象マシンにパッチを適用する．
3. パッチに関連するフィルタリングルールを削除する．
4. パッチ適用後，マシンの動作がパッチ適用前と変らないことを確認するため，マシンの動作確認を行う．

7.3. 通信及びマシン挙動の異変を発見した場合

通信及びマシンの挙動の監視結果から，マシン異変を発見した場合，以下の動作を行う．

1. セキュリティ関連情報とネットワークシステムの情報から，ネットワークシステム内のマシンが被害を受けているかどうかを判断する．
2. 被害を受けていると判断された場合，被害の拡散性や被害規模の推定を行う．
3. 離隔点となるルータを決定する．
4. 離隔点となるルータに離隔情報を送信することによって離隔を命令する．
5. 離隔を確認したら，被害を受けたマシンの修復を行う．

7.4. 新たなマシンが接続された場合１

特定のソフトウェアがインストールされていないマシンが新たに接続された場合，以下の動作を行う．

1. 最も近いルータが新たなマシンの MAC アドレス等によって離隔し，離隔を確認したら新たなマシンに IP アドレスを付与する．
2. セキュリティ関連情報をもとにマシンを診断する．
3. 必要に応じて予防を行い，その後離隔を解除する．

7.5. 新たなマシンが接続された場合２

各ネットワークマシンに IP アドレスがなくてもマシン情報およびフィルタリング情報を送信する機能がインストールされている（例えばブロードキャストを利

用) マシンが新たに接続された場合, 以下の動作を行う.

1. 新たなマシンからの情報とセキュリティ関連情報をもとに新たなマシンを診断する.
2. 診断に合格したら, 当該ネットワークマシンの接続を許可する.

7.6. 新たなハードウェアが接続された場合

機器構成変更通知を送信する機能がインストールされている各マシンが機器構成を変更した場合, 以下の動作を行う.

1. 診断機能が新たなマシンからの情報をもとに機器構成変更情報をチェックする.
2. 許可されていない機器を含んでいたら, 最も近いルータが新たなマシンの MAC アドレス等によって離隔する.

8. 考察

本章では, 提案システムが 3 章で示したセキュリティ管理のための要件を満たしているかについて検討を行う.

(1) 最新のセキュリティ関連情報から適切なものをすばやく入手すること

提案システムでは, 診断機能がセキュリティ最新情報を自動的に取得する. このとき, 定期的に取得を試み, 更新されていれば新たな情報が収集する. よって, 提案システムは最新のセキュリティ関連情報をすばやく収集できるといえる.

(2) ネットワークシステムの構成に関する情報を正確に把握すること

提案システムでは, 診断機能が必要に応じてネットワークシステムの情報を自動的に収集し整理する. よって, 提案システムはネットワークシステムの情報を正確に把握しているといえる.

(3) 迅速かつ適切に対策を導出すること

提案システムでは, 診断, 補修, 防御, 離隔, 修復およびフィルタリングルール作成装置が, セキュリティ関連情報およびネットワークシステムの情報, もしくは, その 2 次的な情報をもとに自動的に対策を導出する. よって, 情報をもとに迅速かつ適切な対策の導出しているといえる.

(4) 複数の対策に対して最善な対策を選択し実施すること

診断機能では, 複数の対策が導出される. ネットワークシステム内には複数の対象マシンが存在するため, これら複数の対策はパラレルに行うことが可能である. よって, 複数の対策に対してマシン毎に最善な対策を選択し実施しているといえる.

9. まとめと今後の課題

本稿では, 不正アクセス等の脅威からネットワークの安全性を自律的に維持するシステムのフレームワークを提案し, 4つのセキュリティ管理のための要件を満たしていることを言及した. また6つのケーススタディを用いて, 事象に対する具体的なフローを示した.

今後の課題としては, セキュリティ関連情報の収集方法や被害を受けたマシンの同定方法等が考えられる. また, 各機能を実装して提案システムのフィージビリティスタディを行うことも必要である.

参考文献

[1] 山田朝彦, 嶋田雄二郎, "自動パッチ配布･適用・管理技術に関する調査", http://www.ipa.go.jp/security/products/fy12/report/H12-Mid-6-1.pdf, 2001.

[2] 三友仁史, 鳥居悟, 小野越夫, "Web サーバ防御ツールの実用性評価", CSEC 研究発表会 (第 15 回), 2001.

[3] 三友他, "Web サーバ向け不正アクセスフィルタの構築", 情報処理学会第 62 回全国大会, Mar., 2001.

[4] Matthew M. Williamson, "Throttling Viruses: Restricting propagation to defeat malicious mobile code", 18th Annual Computer Security Applications Conference (ACSAC), http://www.acsac.org/2002/abstracts/97.html, Dec., 2002.